Annex B:
Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

December 02, 2002
Draft

Jean Campbell
Randall J. Easter
Annabelle Lee
Ronald Tencati

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Annex B: Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following:

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules to FIPS PUB 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE - www.cse-cst.gc.ca) of the Government of Canada. Products validated as conforming to FIPS PUB 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. Organizations wishing to have validations performed would contract with the laboratories for the required services.

2. Purpose

The purpose of this document is to provide a list of the FIPS Approved protection profiles applicable to FIPS PUB 140-2.

Table of Contents

ANNEX B: APPROVED PROTECTION PROFILES

Annex B provides a list of the FIPS Approved protection profiles applicable to FIPS PUB 140-2.

1. *Controlled Access Protection Profile (CAPP),* Version 1.d, Protection Profile NoPP006, 8 October 1999.

2. *Protection Profile for Single-Level Operating Systems in Environments Requiring Medium Robustness*, Version 1.22, 23 May 2001.

End of Document